

BRYAN D. SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West 7th Ave., #9, Rm. 253
Anchorage, AK 99513-7567
Phone: 907-271-5071
Email: adam.alexander@usdoj.gov

KENNETH A. BLANCO
Acting Assistant Attorney General

CATHERINE ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Email: Catherine.Pelker@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA,) No.
)
Plaintiff,) <u>COUNT 1:</u>
) CONSPIRACY TO COMMIT A
vs.) VIOLATION OF 18 U.S.C. § 1030(a)(5)
) Vio. Of 18 U.S.C. § 371
PARAS JHA)
)
Defendant.)

INFORMATION

The United States Attorney charges that:

INTRODUCTION

1. The “Internet” is a global network connecting millions of computers and computer networks to each other, allowing them to communicate and transfer information. Using, among other things, a system of wires, cables, routers and circuits, the Internet allows the communication and transfer of information in interstate and foreign commerce. Computers that are connected to the Internet may come in different forms, from personal computers, laptops and smartphones, to large scale servers that host websites and online services, to more minimal devices such as Internet-connected cameras, digital video recorders (“DVR”) and routers.

2. “Malware” is malicious software designed to damage or disable a computer, or provide control of the computer to a third party.

3. A “botnet” is a collection of computers infected with malware that are controlled as a group, typically without the owners’ knowledge. The individual computers within a botnet, known as “bots,” respond to commands from one or more master computers. These master computers are commonly known as “command and control” (“C2”) computers.

4. “DDOS attacks” occur when multiple computers acting in unison flood the Internet connection of a targeted computer or computers. The overwhelming amount of traffic generated by such an attack quickly overwhelms the capacity of the target computer, resulting in the target computer being unable to send, receive or respond to commands. DDOS attacks are often directed at servers that host websites, with the intent of rendering those websites unavailable to the public.

5. A “proxy” is an intermediary computer server that relays traffic from one computer to another. Proxies are used to obfuscate the Internet Protocol address of the originating computer, which makes online attribution more difficult.

6. Mirai is the name of a malware variant utilized to hijack computing devices to create botnets to facilitate further criminal activity. Unlike previous malware designed to create botnets, Mirai targets the “Internet of Things” (“IoT”) – non-traditional computing devices that have been connected to the Internet, including wireless cameras, routers and digital video recorders.

COUNT 1 (Conspiracy)

7. The allegations set forth in paragraphs one through six of this Information are re-alleged as if fully stated herein.

8. Between in or about July 2016, and continuing thereafter to on or about October 4, 2016, in the District of Alaska and elsewhere, defendant PARAS JHA, and other persons, did knowingly and intentionally conspire and agree with one another to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and to cause loss during a one-year period aggregating at least \$5,000 in value and to cause damage affecting 10 or more protected computers during a 1-year period in violation of 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(A).

//

//

THE OBJECT OF THE CONSPIRACY

9. The object of the unlawful conspiracy was to infect computing devices with the Mirai malware developed by the conspirators for the purpose of enlisting those devices into a botnet that could be used to conduct powerful DDOS attacks and facilitate other criminal activity.

MANNER AND MEANS OF THE CONSPIRACY

10. It was part of the conspiracy that the defendant PARAS JHA and his co-conspirators would attempt to discover both known and previously undisclosed vulnerabilities that would allow them to surreptitiously attain administrative or high-level access to victim devices for the purpose of forcing the devices to participate in the Mirai botnet. Utilizing undisclosed vulnerabilities meant that JHA and co-conspirators would not have to compete with other criminal actors seeking to develop illicit botnets for access to these devices. Devices with such vulnerabilities were compromised by JHA and his co-conspirators without authorization of the owner of the affected devices.

11. It was further a part of the conspiracy that the defendant PARAS JHA and his co-conspirators would scan the internet for vulnerable IoT devices and, without authorization, attempt to gain administrative access to those devices through the use of credentials that they were not authorized to employ.

12. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would, without authorization, infect with Mirai the IoT devices they were able to access, which afforded the defendant PARAS JHA and his co-conspirators complete control over the devices, and hijack them to create the Mirai botnet.

13. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would use their Mirai botnet to conduct powerful DDOS attacks, which caused damage to the servers targeted in the attacks.

14. It was further part of the conspiracy that the defendant PARAS JHA and his co-conspirators would rent access to their Mirai botnet, which enabled other criminals to use the botnet to conduct powerful DDOS attacks. These attacks caused damage to the targeted servers, and were large enough to cause incidental damage to many servers located in close logical proximity to the targeted server. In fact, one feature of Mirai was the ability to conduct attacks against entire ranges of IPs, meaning that a victim's entire network would be affected. This feature, in conjunction with the very large size of the Mirai botnet, rendered useless many methods that are used to mitigate DDOS attacks, meaning that the attacks were capable of causing more network disruption than would be experienced in attacks by other DDOS services.

OVERT ACTS

15. In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the District of Alaska and elsewhere:

- (a) In or about July 2016, defendant PARAS JHA wrote and implemented computer code with his co-conspirators that enabled them to control and direct devices infected with the Mirai malware. Over 300,000 such devices ultimately became part of the Mirai botnet and were used by JHA and others

to unlawfully participate in DDOS attacks and other criminal activity. Some of these devices were located in the District of Alaska.

- (b) From August to September 30, 2016, defendant PARAS JHA conspired to conduct DDOS attacks against websites and web hosting companies located in the United States and abroad.
- (c) In August 2016, while directing a DDOS attack against a U.S. company, defendant JHA contacted the company and demanded payment in exchange for halting the attack.
- (d) From September to October 2016, defendant PARAS JHA publicly promoted Mirai on a variety of forums. Using monikers such as “ogmemes” and “Anna Senpai,” JHA advertised the botnet and discussed its capabilities on discussion boards frequented by cyber criminals. JHA and his co-conspirators actively solicited criminal clients for Mirai, serving as a point of contact for individuals interested in leasing the botnet and negotiating with prospective customers in order to generate illicit proceeds.
- (e) From August to September 2016, defendant PARAS JHA set up and maintained technical infrastructure essential to the operation of Mirai. JHA ran Mirai on virtual machines that operated on his own computer hardware, which he stored and maintained at his family residence.

//

//

- (f) From August to September 2016, defendant PARAS JHA conspired to set up and maintain technical infrastructure relating to the command and control of the Mirai botnet at hosting providers and web optimization services, essential to the operation of Mirai.
- (g) In August 2016, defendant PARAS JHA engaged in a feud with rival DDOS botnet operators, during which period JHA generated and sent fraudulent abuse complaints to hosting providers associated with the rival group. JHA also conspired to conduct DDOS attacks against Internet architecture associated with this group. JHA further participated in a Border Gateway Protocol (BGP) hijacking scheme in which JHA and co-conspirators fraudulently gained control over IP addresses that were in legitimate use by third parties. JHA conducted these activities to consolidate and maximize the power of the Mirai botnet.
- (h) In or about September and October 2017, defendant PARAS JHA took steps to destroy or conceal evidence from law enforcement, in furtherance of the conspiracy. JHA securely erased the virtual machine used to run Mirai on his device. JHA posted the Mirai code online, in order to create plausible deniability if law enforcement found the code on computers controlled by JHA or his co-conspirators.

//

//

All of which is in violation of Title 18, United States Code, Section 371.

RESPECTFULLY SUBMITTED December 5, 2017, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Adam Alexander
ADAM ALEXANDER
Assistant U.S. Attorney
United States of America